REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Status of Present Application

Applicant advises that a Notice of Appeal was filed on October 26, 2006 with a request for a two-month extension of time, and a Brief on Appeal filed on February 19, 2007. A first Notice of Non-Compliant Appeal Brief was issued on April 25, 2007 and an Amended Brief on Appeal submitted on May 9, 2007. A second Notice of Non-Compliant Appeal Brief was issued on August 17, 2007. The present response is being filed concurrently with a request for a two-month extension of time (Sep 17 to Nov 17) and a request for continued examination (RCE) to reopen prosecution. It is believed that the present application should now be taken out of the appeal process and that in view of the present response, the RCE is proper. As such, the above-noted amendments should be entered and prosecution continued on the basis of such amendments.

Personal Interview

Applicant wishes to thank the Examiner's supervisor (Christopher Revak) for taking the time to meet with the undersigned, John Orange (29,725), and Dr. Scott Vanstone in a personal interview on October 18, 2007 and wishes to thank the Examiner for taking the time to meet with the undersigned and Mr. Orange on October 19, 2007 in a follow up interview.

During the first of the personal interviews, proposed amendments were discussed and how such amendments differentiate over the Dworkin reference. It was determined that by emphasizing more clearly in the claim that no reduction takes place on the partial values (sub-steps) and reduction takes place only on the accumulated or intermediate result, the claims would clearly distinguish over Dworkin since Dworkin clearly and explicitly teaches reducing each partial product. The claims have been amended taking these discussions into consideration. The proposed amendments were also discussed with the Examiner in the second personal interview and it is believed that the language used in the amended claims both distinguishes over the Dworkin reference and is fully supported by the specification as filed.

Claim Amendments

Claims 1, 3, 4, 5 and 6 have each been amended along the lines discussed during the personal interview, namely to emphasize that the reduction does not take place until after the result is accumulated or an otherwise intermediate product is obtained. It may be noted that support for the terms "non-reducing" and "unreduced" and the provision of not reducing until the end of the computation can be found on page 12, lines 17-26 and page 16, line 29 through page

17, line 2. No new subject matter is believed to have been added by way of these amendments.

Claim Rejections

Claims 1 and 3-11 have been rejected under 35 U.S.C. 102(a) and 35 U.S.C. 102(e) as being anticipated by Dworkin et al. (US 6,230,179). Applicant respectfully traverses the rejections as follows.

As noted above and discussed at length in the personal interviews, the present application is directed to performing finite field operations by performing non-reducing computations and then a reduction at the end, which increases randomness, is more efficient (e.g. may only need to perform one reduction for an entire operation) and inhibits side-channel attacks. Claims 1, 3, 4, 5 and 6 have been amended to emphasize that the reduction is not performed until the end of the operation, which, as discussed in the personal interviews clearly distinguishes over the Dworkin reference.

In Dworkin, what is commonly referred to as full reduction is performed where each partial product is reduced (see col. 4, lines 32-34 and col. 10, lines 43-53).

Accordingly, the claims, as amended, are believed to clearly and patentably distinguish over Dworkin and are believed to be in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,

Brett J. Slaney
Agent for Applicant
Registration No. 58,772

Date: October 30, 2007

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416-863-2518
BS/